Cal-CSIRS FAQ

Answers to Frequently Asked Questions (FAQ)

1. **What if I am in multiple roles for multiple entities?**
   You will be issued a single user-id and password that can connect to each of your entities.

2. **What if my entity needs more than one alternate reporting designee who can report incidents?**
   Unfortunately we are unable to accommodate the request for additional user accounts at this time. We are able to provide each state entity with a total of three Cal-CSIRS user accounts. One account will be assigned to the designated Chief Information Officer (CIO) and one account will be assigned to the designated Information Security Officer (ISO). The entity may choose one alternate designee for the third account. To ensure that the CISO office is providing access to accommodate the assigned reporting structure, it is crucial that we provide the primary CIO and the primary ISO access into the Cal-CSIRS system.

   CIOs and Information Security Officers (ISOs) are designated by their Directorate (entity head) in accordance with legal and policy requirements (Government Code 11546 and SAM 5330), and are responsible for keeping their Directorate informed of risk and incident related matters. Therefore we are ensuring that all the primary CIO and ISO designees have access to the Cal-CSIRS reporting system and one alternate of the entity's choosing are able to access information reported on behalf of their entity and the management report capabilities so that these individuals will be able to keep their Directorate fully informed.

   We understand the need for additional user accounts and are looking into an enterprise licensing approach that may accommodate additional user accounts in the future. Please feel free to contact our office if you have further questions.

3. **Will our AIO and AISO have access to all of the Departments included within their Agency?**
   Yes, the security model is designed to segregate the agencies and department views.

4. **How do I change the selected alternate reporting designee?**
   If the alternate reporting designee information needs to be changed, notification must be made by the CIO or ISO to CISO at security@state.ca.gov. Our Office will provide you with the Cal-CSIRS reporting designation form and instructions.

   Note: The Cal-CSIRS reporting designation form is separate from the annual Agency Designation Letter (SIMM 5330-A) and facilitates access and authentication preferences for Cal-CSIRS. If you have a change in your CIO or ISO designation you will still use the SIMM 5330-A.

5. **How does my new designee obtain the Cal-CSIRS User Manual?**
   When a completed Cal-CSIRS reporting designation form is submitted to our Office, a Cal-CSIR User Manual will be sent to the new reporting designee.

6. **Is there a new incident number scheme for Cal-CSIRS?**
   Yes, Cal-CSIRS has a new number scheme.

7. **Will previous SIMM 5340-B incidents be uploaded into Cal-CSIR?**
   No. It is not feasible to import CHP and CISO data from existing and disparate reporting systems to the new system. We will implement a clean cut-over from the old reporting process to the new Cal-CSIRS reporting process.

8. **If California Highway Patrol (CHP) Computer Crimes Investigations Unit (CCIU) decides to investigate will they or the Emergency Notification and Tactical Alert Center (ENTAC) give me a separate number for the same incident?**
   CHP will use the Cal-CSIRS number; thus, CHP and CISO will now use the same number.

9. Will an entity be able to print an individual incident report?
Yes. Initially the individual report will print all possible questions and any answers to those questions.

10. Will an entity be required to print and route a hard-copy of the report for signatures?
No, with the implementation of Cal-CSIRS, routing a hard-copy for signatures will no longer be required. State entities must continue to inform their Privacy Officer, CIO and department director of incidents in accordance with state policy on incident handling and coordination (SAM 5340.3 and SAM 5340.4) instructions and procedures (SIMM 5340-A) as well as in accordance with their internal organizational processes and procedures. Further, the system will allow entities to create reports of open and closed incidents to facilitate Security Governance and Executive Management briefings.

11. Will Cal-CSIRS generate either the Std 152 or Std 99 form?
Cal-CSIRs will allow you to print the data input into Cal-CSIRS to assist with preparing those reports. However, because those reports require much more information than Cal-CSIRS requires, you will still need to complete the Department of General Services Std 152 and California Highway Patrol Std 99 forms if applicable to the incidents you report through Cal-CSIRS, and send them to DGS and CHP.

12. Will Two Factor Authentication (2FA) be required to access Cal-CSIRS?
Yes. State entities will provide Cal-CSIRS user contact information for receiving the randomly generated code to our Office through the Cal-CSIRS reporting designation process. At login, the system will generate a one-time code to enter along with user id and password.

13. Will 2FA be required each time a user logs into Cal-CSIRS?
No. 2FA will only be required once during the day if you are logging in/out/in on the same device.

14. Since each profile is tied to their role (AIO, ISO for example) and the departments and/or agencies that they will have privileges for, why can't the profile be further customized and automatically answer some questions, which could be overridden if necessary. For example, if I am a department that does not have HIPAA requirements, why can't that question be automatically be set to "no" for my profile?

This is not currently part of the profile but we understand the need to continue to simplify wherever possible. A Cal-CSIRS user group will be established to facilitate identification, prioritization and general governance of future changes and enhancements.

15. What will be the retention policy for incidents in Cal-CSIRS?

It will be in accordance with our Department's current retention policy for these records, which is currently 5 years from the date an incident is closed.

16. Is the data in Cal-CSIRS subject to Public Records Act (PRA) requests, or exempt from PRA pursuant to Government Code Section 6254.19

Yes, these records are subject to PRA requests. However, some data within Cal-CSIRS may be considered confidential and exempt from disclosure. For example, records for which the disclosure of that record would reveal vulnerabilities to, or otherwise increase the potential for an attack on, an information technology system of a public agency (Government Code Section 6254.19). The Department's process is to review all requested records and redact when necessary the protected or otherwise exempt portions of the record before its release.

17. What is the "Situational Awareness" button?

The situational awareness button allows a reporter to share information about anomalous or suspicious activity they've observed that has not risen to a reportable incident for their entity. As an example, a large department may wish to share that it is seeing an unusually high volume of traffic from a specific IP or IP range. The situation may not have resulted in an outage or disruption but could impact others and would be worth sharing. To create a Situational Awareness Report use the "Situational Awareness" button instead of the "Submit" button.

18. Who can see and who is notified when the Situational Awareness reports made through Cal-CSIRS?

All Cal-CSIRS users may see a Situational Awareness report. The SAR allows the community to share information about suspicious activity trends and anomalies (for example an uptick in probe and scan activity) that may not constitute a reportable incident.

19. Who can see and is notified when a department submits an incident report?

Authorized representatives from CHP's Emergency Notification and Tactical Alert Center (ENTAC) and Computer Crime Investigations Unit (CCIU), authorized representatives from the California State Threat Assessment Center system, and authorized representatives from the California Information Security Office (CISO), and authorized users in the reporting entity and its Cabinet-level Agency may see reports submitted by a department. Cabinet-level agencies have visibility of all entities reporting up to them. An email alert is sent only to authorized representatives from CHP's Emergency Notification and Tactical Alert Center (ENTAC) and Computer Crime Investigations Unit (CCIU), authorized representatives from the California State Threat Assessment System, and authorized representatives from the California Information Security Office (CISO) when an incident is reported. Once reviewed by CISO an acknowledgement is sent to the reporting entity.

20. How will communications occur between CISO and reporting entities?

Cal-CSIRS is an incident reporting system not an incident management system. Conversations needed to manage incident response will still need to occur by telephone, but these can be documented and preserved as part of the report record in the workflow notes, and notes/comments fields.

21. How will communications occur between CCIU and reporting entities?

Cal-CSIRS is an incident reporting system not an incident management system. Conversations needed to manage incident response will still need to occur by telephone, but these can be

documented and preserved as part of the report record in the workflow notes, and notes/comments fields.

22. I am an authorized reporting designee for my Agency, may I submit an incident on behalf of a department that reports up to our Agency?

Yes. Please contact CISO if you need assistance with doing so.

23. I am an authorized reporting designee for my Department, may I submit an incident on behalf of another state department that we have an information exchange or system interconnection with business relationship with?

No, the other department's authorized reporting designee will need to report the incident.

24. How is an incident closed?

CISO will review reported incidents for completeness and will work with reporting entities to determine when they may be closed. Authorized reporters/preparers may update information in the system as it becomes available using the Save and Close button. Once the entity believes all required information has been entered they may select the Final Update button and this will send a notice to CISO

25. May we add additional information after an incident is closed?

No. If needed, you may contact the CISO to make the needed comment/note.

26. How do we report an incident if Cal-CSIRS is offline?

You will contact the California Information Security Office (CISO) during business hours to report the system is offline, and you or a CISO representative will enter your report once the system is back online. **<u>If</u> after regular business hours** you require immediate law enforcement assistance you will contact the CHP's Emergency Notification and Tactical Alert Center (ENTAC) at (916) 843-4199. **Note: ENTAC is only to be contacted when immediate law enforcement assistance is needed after regular business hours.**

27. What is the Risk Assessment tab?

Cal-CSIRS is designed to be a fully integrated governance, risk and compliance reporting system. The Risk Assessment module is for future use and has not yet been enabled.